# WLAN Security Threats & Solutions

Franjo Majstor, Senior Consulting Engineer
Cisco Systems, Brussels, Belgium

## Abstract

*This session will give an overview of the latest security trends in the 802.11 based WLAN technology. WLAN technology in security terms had a hard start with early discovery of multiple weaknesses built into it by the design, or discovered afterwards by the inappropriate use of the crypto technology. Initial development of the WEP (Wire Equivalent Privacy) protocol had missed to address the key exchange mechanism as well as individual user authentication. On top of that it does not provide either crypto integrity checking mechanism or replay protection.*

*Immediately after their discovery and public announcements most of the mentioned weaknesses also got publicly available tools on the Internet for their testing and unfortunately, also possible abuse. There are currently two solution paths in industry for securing the WLAN technology. IEEE and IETF standardization bodies have already developed and proposed multiple protocols such as 802.1x and multiple new EAP's (Extended Authentication Protocol) to address security weaknesses in the user authentication and the lack of a key management. The IEEE TGi (Task Group i) is working on a comprehensive solution within the 802.11i standard to address all of the existing security weaknesses of the WLAN technology. Another industry initiative, driven by the leading WLAN technology vendors, have adopted a subset of the TGi work under name of WPA (Wi-Fi Protected Access) to overcome the time limitations in long standard developments, and apply changes and fixes which are immediately possible to address the most important security weaknesses of a current WLAN technology.*

## About the speaker

**Franjo Majstor, *Senior Consulting Engineer, Cisco Systems, Brussels, Belgium***

Franjo Majstor holds an University Graduate Engineering degree from the Faculty of Electrical Engineering at University of Zagreb, Croatia and Master of Science degree obtained on subject "IPsec Extensions" from the Faculty of Computer Sciences at KUL University of Leuven, Belgium. He started his industry career back in 1990 in Slovenia, in 1995 joined Cisco Systems, Inc. in Belgium, where he is currently working out of Brussels office.

In his role of a senior technical consultant, he is focusing on security products, features and solutions across technologies and is involved as a trusted adviser in designs of major network security related projects in Europe, Middle East and Africa. He holds a CISSP (Certified Information Systems Security Professional) certification from (ISC)2 (International Information Systems Security Certifications Consortium) and CCIE (Cisco Certified Internetworking Expert) in security and access areas from Cisco Systems, Inc. He is also a member of several professional associations: CSI (Computer Security Institute), ISSA (Information System Security Association), IEEE, IETF and is a frequent speaker at worldwide technical conferences on network security topics.

## About Cisco Systems

Cisco Systems, Inc. is the worldwide leader in networking for the Internet. Cisco's Internet Protocol-based (IP) networking solutions are the foundation of the Internet and most corporate, education, and government networks around the world. Cisco provides the broadest line of secure solutions for transporting data, voice and video within buildings, across campuses, or around the world.

Cisco Systems chairs the IEEE 802.11i task group on MAC Enhancements for Enhanced Security (Dave Halasz), which is working on producing a standard that will further improve Wireless LAN security (for more info see the TG-info web page at http://grouper.ieee.org/groups/802/11/Reports/tgi_update.htm). Furthermore, Cisco participates in the IEEE 802.11e task group on MAC Enhancements for Quality of Service.

Proceedings of the 28th Annual IEEE International Conference on Local Computer Networks (LCN'03)
0742-1303/03 $ 17.00 © 2003 IEEE